

EXHIBIT C



DATA SECURITY & INFORMATION PRIVACY POLICY

Policy Area	Employee Handbook: Data Security & Information Privacy Policy
Approved Date	October 12, 2023
Approved By	Director of Information Technology – Joel Prest; CFO, COO – James Hardy
Effective Date	October 12, 2023
Current Version	7.0

I. OVERVIEW

Atticus Administration, LLC ("Atticus"), in fulfilling the requirement as a third-party administrator under the terms of a court order and/or settlement agreement for a case ("Case Court Documents"), is required to collect and store client information such as class member data records which contain names, addresses, phone numbers, emails, and occasionally sensitive information such as social security numbers, and takes seriously its obligation to secure information systems and protect the privacy of this client data.

As a standard operating procedure, Atticus regularly reviews its policies related to data collection, privacy, and security. All who are employed by Atticus or retained as a contractor for Atticus ("Users") are provided with this Data Security & Information Privacy Policy document as a part of their training or onboarding to ensure that this information is communicated and understood through explicit acknowledgment. Any material revisions to this document are immediately communicated to Users with an emailed memo which calls out the revisions, as well as an updated copy of the Data Security & Information Privacy Policy document.

Atticus complies with the policies and processes encompassed within this Data Security & Information Privacy Policy document.

II. PURPOSE

The purpose of this Policy is to establish the rules for handling the collection, storage, and use of client data. These rules are necessary to preserve the integrity, availability, and confidentiality of information.

III. SCOPE

This policy applies to all Atticus employees and contractors that use company assets such as computers, laptops, or mobile devices and/or have access to Atticus' networks and information resources. All devices, whether owned by Atticus or owned by employees, that have access to Atticus' networks and information resources are governed by this Data Security & Information Privacy Policy. Usage of applications, including cloud storage software, by employees on their own personal devices, are also subject to this policy.

IV. POLICY

1. Data Governance

Atticus is committed to protecting and safeguarding the data that it collects and recognizes this data as a critical asset. Atticus maintains a tiered data governance structure, managed by the Director of Information Technology and enforced by Atticus executive leadership, that governs individual Users access to data. This governance structure is further maintained through enforced processes, standards, and procedures to ultimately ensure appropriate use of data and/or management of data.

**2. Internal Use of Data**

Any client data and class member data records that Atticus collects, and stores are used only to fulfill Atticus' requirement as a third-party administrator under the terms of the Case Court Documents. This information is only available to Users as set forth by Atticus' tiered data governance structure.

3. External Use & Disclosure of Data

Atticus follows the direction and instructions outlined in the Case Court Documents for handling class member data records. All sensitive and non-public client data, class member data, and information for a case that is provided to Atticus, is the property of Atticus and may not be shared, used, or otherwise communicated outside of Atticus or outside the scope of the project. In cases where a contractor partner is used, only those who have been approved and authorized by Atticus management and have a privacy policy (or data security policy) consistent with Atticus' Data Security & Information Privacy Policy are allowed to be used.

4. Data Security & Information Privacy Policy

Electronic transmission, delivery or receipt of sensitive data is only permitted using SFTP technology. Delivery or receipt of hardcopy sensitive data is only permitted using the US Mail System or a courier as approved by Atticus management.

Atticus complies with all state and federal regulations that apply to data security.

Once a case has closed, Atticus will destroy all hardcopy documents containing sensitive data within twelve months. Regarding all electronic case data (including sensitive data), Atticus maintains this data for up to five years following the closure of the case. In the event Court Case Documents specify unique data retention/return requirements, those requirements shall prevail over Atticus' standard retention/return policy.

5. Computing Devices & Access to Atticus Information Database and Network

Only Atticus IT approved devices may be used to access Atticus' information database and network. All devices must be protected with an employee's user access level systems username and password required at the time the device is powered on.

Access to database and network information must be authenticated using two-factor authentication.

Sensitive data shall not be stored on the device. However, in the event there is no alternative to device storage, all sensitive data must be encrypted with password protection.

Atticus prohibits the use of public cloud storage for any client specific data.

Unattended devices must be logged out and locked when unattended, and additionally configured to automatically be logged out of and screen locked after 10 minute or more of inactivity.

All devices that access Atticus' information database and network infrastructure shall have active and up-to-date anti-malware and firewall protection.

6. Breaches in Security and Policy Violation

Breaches in security, whether actual or suspected, must be reported immediately to Atticus' Director of Information Technology. The Director of Information Technology and executive management will assess the breach for scope and severity and take appropriate action to mitigate and/or eliminate.



ATTICUS

1250 NORTHLAND DRIVE SUITE 240
MENDOTA HEIGHTS MN 55120
WWW.ATTICUSADMIN.COM
1-844-728-8428

If the Director of Information Technology and/or executive management, is made aware a User has failed to comply with Atticus' Data Security & Information Privacy Policy, they will identify and apply appropriate consequences to the User. Consequences may be as severe as termination of employment or termination of contract and/or further legal action. If there is a concern about a breach involving the Director of Information Technology, concerns should be immediately directed to the Chief Operating Officer.

If there is a data breach with a vendor/contractor, the contractor must comply with all applicable state and federal laws that require the notification to individuals (or other affected parties) in the event of unauthorized release of sensitive personal information or confidential data. Contractors must notify Atticus within 24 hours of the incident. Atticus reserves all rights to act under the terms of any applicable contract, including indemnification and/or termination of the contract.

7. General Atticus Information Security and Privacy Standards

- **Annual security training.** Training and review of the Information Security and Privacy Standards are provided to Atticus Employees on an annual basis. Periodic security reminders may be used to reinforce computing device security procedures, updates, or changes.
- **Minimum necessary.** Employees shall only have access to the minimum amount of data necessary to perform their job duties.
- **Lost devices.** Employees must immediately report any lost or stolen devices so access to systems can be deactivated.
- **Unauthorized access.** Any unauthorized access to a device or company data must be immediately reported.
- **Rooting Mobile computing devices.** Mobile computing devices must not be "rooted" or have unauthorized software/firmware installed. A mobile device is considered "rooted" if the internal protections of the device have been compromised or modified to allow control access to the operating system.
- **Content.** Employees shall not load illegal content or pirated software onto devices.
- **Software installs.** Only approved applications are allowed on the computing devices that connect to Atticus' information database and network.
- **Patch management.** Computing devices and applications must be kept up-to-date. Patches should be installed within 30 days of release.
- **Anti-malware.** All computing devices must have active and up-to-date anti-malware protection software. encryption. Encryption shall be used to protect sensitive information.
- **Firewalls.** Firewall is maintained at the headquarters location for the network and administered by the Director of Information Technology.
- **Work habits.** Employee shall use Atticus company applications and systems while at work. Access to certain outside applications, websites, and/or systems may be blocked within each Atticus computing device.
- **Backups.** Backups are performed twice daily on the network terminal server environment.
- **Internal applications.** Computing devices are installed with company internal applications on an as needed basis to Users. User access rights are maintained by the Director of Information Technology.
- **Exemptions.** A risk assessment and risk analysis shall be performed for any requests for exemptions from this Policy.

V. ENFORCEMENT

Any User found to have violated this policy may be subject to disciplinary action. Such action may be as severe as termination of employment or termination of contract and/or further legal action.

VI. DISTRIBUTION



ATTICUS

1250 NORTHLAND DRIVE SUITE 240
MENDOTA HEIGHTS MN 55120
WWW.ATTICUSADMIN.COM
1-844-728-8428

This policy is to be distributed to all Users.

Policy History

Version	Date	Description	Approved By
1.0	8/1/2017	Initial policy release	Mai Vang – Director of Operations James Hardy – CFO/COO
2.0	11/5/2018	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO
3.0	11/14/2019	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO
4.0	11/10/2020	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO
5.0	10/15/2021	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO
6.0	10/12/2022	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO
7.0	10/12/2023	Policy Review	Joel Prest – Director of Information Technology James Hardy – CFO/COO